Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

32 761 Verwerking en bescherming persoonsgegevens

Nr. 641

BRIEF VAN DE MINISTER VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 oktober 2019

1. Aanleiding

Data-analyses bieden veel kansen voor bedrijven en overheden om hun zaken efficiënter en effectiever in te richten. Zo kan een bedrijf met behulp daarvan betere klantprofielen maken. Overheidsorganisaties kunnen daarmee bijvoorbeeld risicotaxatiemodellen inrichten waarmee zij beter toezicht kunnen houden op de naleving van wet- en regelgeving of efficiënter fraude kunnen opsporen. Digitalisering zorgt er daarbij voor dat er ook steeds meer en betere mogelijkheden ontstaan om data te vergaren en te analyseren.

Data-analyses geven ook risico's. De transparantie rond data-analyses kan onvoldoende zijn. Hierdoor weten burgers vaak niet dat zij onderwerp zijn van een data-analyse, waarvoor die analyse wordt gemaakt en de precieze effecten daarvan. Door dit gebrek aan transparantie weet men zich niet goed te weren tegen de uitkomsten van zo'n analyse. De groeiende complexiteit van analysemethodes en daarbij gebruikte algoritmes maakt ook dat de analyses en de uitkomsten daarvan steeds lastiger te doorgronden zijn en daardoor ook moeilijker te controleren. Daarnaast bestaat het risico op onregelmatigheden in de datasets of algoritmes. Zo kunnen datasets bias bevatten die in de data-analyse gereproduceerd worden. Ook kunnen er discriminerende effecten optreden wanneer (onbedoeld) vooroordelen van experts worden vertaald in het ontwerp van het algoritme, de keuze van variabelen of de classificatie van gegevens. Bij data-analyses gebaseerd op profilering kan men bijvoorbeeld ten onrechte een bepaalde eigenschap toegekend krijgen (*false positive*) of andersom ten onrechte een eigenschap niet toebedeeld krijgen (*false negative*).

Algoritmes zijn dus niet altijd neutraal, noch hebben ze altijd gelijk. Maar het alternatief waarin afwegingen door de mens worden gemaakt, is evenmin neutraal of altijd juist. Door te kijken naar patronen en verbanden in data zijn we juist in staat om bestaande vooroordelen bloot te leggen

kst-26643-641
ISSN 0921 - 7371
's-Gravenhage 2019

en besluitvorming te objectiveren. Dat neemt niet weg dat het zaak is om voornoemde risico's te onderkennen en waar mogelijk te verminderen.

Tegen deze achtergrond heeft het vorige kabinet in zijn standpunt op het rapport «Big Data in een vrije en veilige samenleving» van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) aangekondigd te bezien of de waarborgen rond het uitvoeren en gebruiken van data-analyses door de overheid kunnen worden versterkt.[1] Vervolgens heb ik tijdens het Algemeen Overleg over Big Data en de bescherming van persoonsgegevens op 30 mei 2018 toegezegd uw Kamer te informeren over mogelijke wettelijke waarborgen om risico's van data-analyses door de overheid tegen te gaan.[2] Met deze brief geef ik mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (BZK) uitvoering aan deze toezegging.

Deze brief staat niet op zichzelf. Zij borduurt voort op mijn brief van 9 oktober 2018 over transparantie van algoritmes in gebruik bij de overheid[3], de kabinetsreactie van 2 november 2018 op het advies van de Raad van State over de effecten van digitalisering voor de rechtstatelijke verhoudingen[4], mijn brief van 19 december 2018 over artificiële intelligentie en algoritmen in de rechtspleging[5], de brief van de Staatssecretaris van BZK van 21 december 2018 over het gebruik van algoritmes door overheden[6] en de kabinetsreactie van 28 maart 2019 op het onderzoeksrapport «Algoritmes en grondrechten» van de Universiteit Utrecht (UU).[7]

Tegelijkertijd met deze brief zijn het Strategisch Actieplan voor Artificiële intelligentie (AI) (SAPAI) (Kamerstukken 26 643 en 32 761, nr. 640) en de beleidsbrief AI, publieke waarden en mensenrechten aan uw Kamer aangeboden. De drie brieven focussen op verschillende onderdelen van het brede vraagstuk ten aanzien van het benutten van kansen en het adresseren van risico's van AI. SAPAI bevat de overkoepelende AI-aanpak van dit kabinet en bevat beleidsmaatregelen om de maatschappelijke en economische kansen van AI te benutten en daarbij de publieke belangen te borgen. SAPAI gaat in spoor 3 kort in op de effecten van AI op publieke waarden. Omdat de effecten van AI op publieke waarden en mensenrechten complex zijn en in potentie ook significant, heeft het kabinet ervoor gekozen om in de brief over AI, publieke waarden en mensenrechten nader aandacht te besteden aan beleid op dit vlak. Ditzelfde geldt voor de onderhavige brief die in het bijzonder ingaat op mogelijke waarborgen tegen de risico's van het gebruik van algoritmes en data-analyses door de overheid.

Op het terrein van AI en algoritmes vormen «transparantie, toetsbaarheid en rechtsbescherming» belangrijke aspecten. Omdat verantwoordelijkheden voor deze aspecten bij verschillende bewindslieden liggen, acht het kabinet het van belang om de respectievelijke verantwoordelijkheden van de bewindspersonen goed te duiden.

---

[1] WRR, Big Data in een vrije en veilige samenleving, 2016. Zie ook Kamerstukken 26 643 en 32 761, nr. 426, p. 9.
[2] Kamerstukken 26 643 en 32 761, nr. 543, p. 39.
[3] Kamerstuk 26 643 en 32 761, nr. 570.
[4] Kamerstuk 26 643, nr. 578. Kamerstukken 26 643 en 32 761, nr. 570.
[5] Kamerstuk 34 775 VI, AH.
[6] Kamerstuk 26 643, nr. 588. Deze brief betreft een reactie op een onderzoek naar het gebruik van algoritmes door overheidsorganisaties, en had in die zin een andere strekking dan de onderhavige brief.
[7] M.J. Vetzo, J.H. Gerards en R. Nehmelman (2018), Algoritmes en grondrechten, p. 143–144; aangeboden aan de Tweede Kamer als bijlage bij: Kamerstuk 26 643, nr. 553.

Algemeen en systeemverantwoordelijk voor (normering rond) transparantie, toetsbaarheid en rechtsbescherming in het kader van AI/algoritmes is de Minister voor Rechtsbescherming. Binnen dit algemene systeem is specifiek verantwoordelijk voor (normering rond) transparantie, toetsbaarheid en rechtsbescherming:

- de Minister voor Rechtsbescherming in relatie tot het algemeen bestuursrecht, het gegevensbeschermingsrecht en het rechtsbestel,
- de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties in relatie tot het openbaar bestuur en
- de Staatssecretaris van Economische Zaken en Klimaat in relatie tot het bedrijfsleven en consumentenbescherming.

Daarnaast is elke bewindspersoon uiteraard verantwoordelijk voor het beleid met betrekking tot AI en algoritmes op het eigen beleidsterrein.

2. Belang, karakter en evaluatie waarborgen

Het staat voor het kabinet voorop dat bij de verdere ontwikkeling en toepassing van data-analyses gebaseerd op algoritmes tegelijkertijd moet worden geïnvesteerd in de ontwikkeling van waarborgen die de hierboven geschetste risico's moeten beperken. Dat draagt immers bij aan het noodzakelijke vertrouwen in deze toepassingen.[8] Volgens het kabinet is de bestaande regelgeving, waaronder de Algemene verordening gegevensbescherming (AVG), onvoldoende toegespitst op het specifieke karakter van data-analyses gebaseerd op algoritmes om deze risico's voldoende te beperken en is het nodig om hiervoor aanvullende waarborgen te realiseren.[9]

Uit de eerder beschreven risico's vloeit voort dat de waarborgen waarmee data-analyses omgeven moeten worden, erop gericht moeten zijn de transparantie van de gebruikte data, algoritmes en analysemethoden te vergroten en de kwaliteit en betrouwbaarheid daarvan te verbeteren. Hiertoe heeft het kabinet waarborgen voor ogen die in eerste instantie het karakter van richtlijnen hebben, maar het wil daarnaast op termijn ook toewerken naar waarborgen die in wetgeving worden opgenomen.

In lijn met de reactie op het WRR-rapport concentreert het kabinet zich in dit stadium op waarborgen voor data-analyses door overheidsorganen. Aangezien veel bedrijven grensoverschrijdend opereren lijkt het niet effectief om ook voor hen waarborgen op nationaal niveau te regelen. Het grensoverschrijdende karakter van vele bedrijfsactiviteiten en -verwerkingen en het principe van vrij verkeer van persoonsgegevens, dat een van de doelstellingen is van de AVG, brengen bovendien met zich dat eventuele wettelijke waarborgen voor data-analyses door het bedrijfsleven beter op Europees niveau kunnen worden vastgesteld.[10] Overigens zijn in Europees verband op dit vlak al initiatieven ontwikkeld.[11]

---

[8] Zie in die zin ook mijn brief van 9 oktober 2018 over transparantie van algoritmes in gebruik bij de overheid.

[9] Hetzelfde geldt voor andere wetten, zoals de Wet openbaarheid van bestuur en de Algemene wet bestuursrecht (Awb).

[10] Zie artikel 1, derde lid, AVG.

[11] De Europese Commissie heeft in april 2018 een Europese strategie gepubliceerd voor Kunstmatige Intelligentie of Artificiële Intelligentie (COM (2018), 237). In december 2018 heeft de Commissie, samen met de lidstaten, een gecoördineerd actieplan AI opgesteld. Op 8 april 2019 zijn de door een Europese High-level Expert Group voorbereide Richtlijnen voor de ontwikkeling en het gebruik van AI (*Ethics Guidelines for Trustworthy AI*) gepubliceerd. Het Kabinet heeft de Kamer hier eerder over geïnformeerd. (https://www.parlementairemonitor.nl/9353000/1/j9vvij5epmj1ey0/vkvlkydt9vmt).

2.1. Richtlijnen

Het kabinet heeft in eerste instantie richtlijnen ontwikkeld voor het toepassen van algoritmische data-analyses.[12] De technologie met betrekking tot data-analyses is voortdurend in ontwikkeling en zal dat ook nog wel blijven. Dit betekent dat sommige waarborgen het best het karakter kunnen krijgen van richtlijnen, die flexibel kunnen worden aangepast aan de technologische ontwikkelingen. Het kabinet heeft daartoe de als bijlage bij deze brief opgenomen «Richtlijnen voor het toepassen van algoritmes door overheden» ontwikkeld.[13] Deze richtlijnen zijn relevant voor data-analyses in brede zin en bevatten concrete en op de stand van de technologie afgestemde aanwijzingen, bedoeld om het inzicht in, de transparantie en de kwaliteit van algoritmes en data-analyses door overheidsinstanties te vergroten. Deze richtlijnen zijn voorbereid in overleg met experts uit diverse uitvoeringsorganisaties en mede gebaseerd op de bestaande praktijk van deze organisaties. Het gaat hier om waarborgen met betrekking tot:

- Bewustzijn risico's,
- Uitlegbaarheid,
- Gegevensherkenning,
- Auditeerbaarheid,
- Verantwoording,
- Validatie,
- Toetsbaarheid,
- Informatievoorziening aan het publiek.

Omdat het hier gaat om een materie die relatief nieuw is, voortdurend in ontwikkeling is en gevolgen heeft voor de uitvoeringspraktijk van vele overheidsorganisaties, acht het kabinet het aangewezen dat de richtlijnen in een vervolgtraject nader worden uitgewerkt en getoetst op hun effectiviteit en uitvoerbaarheid. Hiertoe zal het kabinet het overleg met relevante overheidsorganisaties zoals de politie, Inspectie SZW, UWV en de Belastingdienst, alsook met de VNG en de gemeenten voortzetten. Ook zullen de richtlijnen aan de hand van concrete casussen worden getest in het Transparantielab dat door BZK is ingericht. Daarnaast zal onder auspiciën van de VNG een impactanalyse voor gemeenten worden uitgevoerd. De uitkomsten van een en ander zullen worden betrokken bij een evaluatie van de richtlijnen die kort na de zomer van 2020 zal worden afgerond. Op grond van de resultaten van deze evaluatie zullen de richtlijnen zo nodig worden aangepast of aangescherpt.

2.2. Wettelijke waarborgen

Naast voornoemde richtlijnen wil het kabinet toewerken naar waarborgen die in wetgeving kunnen worden opgenomen. Het voordeel van wettelijke waarborgen, boven (niet-dwingende) richtlijnen, is dat het toezicht op en handhaving van deze waarborgen hiermee worden versterkt.[14] Daarbij kan worden gedacht aan waarborgen die afgeleid zijn uit de richtlijnen en die op basis van de eerder genoemde evaluatie voldoende zijn uitgekristalliseerd om in wetgeving op te nemen.

---

[12] Ook deze richtlijnen vloeien voort uit actiepunten genoemd in de kabinetsbrief van 11 november 2016. Met deze richtlijnen wordt eveneens uitvoering gegeven aan de recente moties van de leden Middendorp en Drost en van de leden Verhoeven en van der Molen, voor zover daarin om dergelijke richtlijnen wordt gevraagd (Kamerstuk 35 200 VII, nr. 14 en Kamerstuk 26 643, nr. 610).

[13] Voor een nadere uiteenzetting van het proces van totstandkoming, karakter en reikwijdte van deze richtlijnen, zie bijlage, onder Inleiding. Raadpleegbaar via www.tweedekamer.nl

[14] Zie hierover onder paragraaf 4. Toezicht en verantwoording.

Daarnaast heeft het kabinet waarborgen voor ogen, waarvoor noodzakelijk is dat die bij wet geregeld worden. Een voorbeeld betreft het voorstel om toe te staan dat bij de ontwikkeling van algoritmische modellen bijzondere persoonsgegevens worden verwerkt, voor zover nodig om discriminerende effecten tegen te gaan. Gelet op het verbod op verwerking van bijzondere persoonsgegevens kan een dergelijke uitzondering alleen in wetgeving worden geregeld.[15]

Als het gaat om wettelijke waarborgen acht het kabinet het voorts aangewezen om de focus te leggen op data-analyses waarbij persoonsgegevens worden verwerkt. De risico's van data-analyses lijken dan het grootst: data-verwerkingen kunnen in dat geval bij uitstek inbreuk maken op de privacy en andere rechten van individuen. Daarbij zoekt het kabinet aansluiting bij de AVG en de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn).[16] Beide regelingen gaan in op »profilering» waarbij juist de risico's zich kunnen voordoen zoals die hierboven zijn beschreven. Aansluiting bij het begrip «profilering» heeft in dit opzicht de voorkeur boven gebruik van het begrip «Big Data», omdat daarvan geen eenduidige definitie bestaat.[17]

Enkele risico's van profilering zijn ook aanwezig bij sommige data-analyses waarbij weliswaar sprake is van verwerking van persoonsgegevens, maar die niet in een evaluatie van een of meer personen uitmonden en om die reden buiten de AVG/Richtlijn-definitie van profilering vallen. Te denken valt aan risicoanalyses die zich niet richten op een persoon, maar op geografische gebieden, zoals een wijk of straat (hierna: gebiedsgebonden analyses). Zulke analyses kunnen bijvoorbeeld tot doel hebben het doen van een voorspelling over de (verhoogde) kans dat een strafbaar feit wordt gepleegd in een bepaald gebied in een bepaalde tijdsperiode.[18]

Samenvattend kiest het kabinet ervoor om wettelijke waarborgen te realiseren voor twee typen data-analyses door de overheid, te weten:
- Profilering, in de betekenis die daaraan wordt gegeven in de AVG en Richtlijn;
- Gebiedsgebonden analyse waarbij ook sprake is van verwerking van persoonsgegevens en van soortgelijke risico's als die welke zich bij profilering voordoen.

Zie voor een toelichting op beide typen gegevensanalyses de desbetreffende bijlage bij deze brief[19].

3. Mogelijke waarborgen

De waarborgen die het kabinet voor ogen staan, zijn, zoals gezegd, erop gericht de transparantie van de gebruikte data, algoritmes en analysemethoden te vergroten en de kwaliteit en betrouwbaarheid daarvan te

---

[15] Zie hierover onder 3.2. Kwaliteitswaarborgen, onder vi. Verwerking bijzondere persoonsgegevens.

[16] Richtlijn (EU) 2016/680 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. Deze Richtlijn is geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).

[17] Zie hierover rapport WRR, p. 33–35, en rapport UU, p.15–16.

[18] Zie hierover ook: Vetzo c.s., p. 26–27, onder *Predictive policing*.

[19] Raadpleegbaar via www.tweedekamer.nl

verbeteren.[20] Het betreft in de eerste plaats waarborgen die als richtlijnen zijn opgenomen in een bijlage bij deze brief en daarin nader zijn uitgewerkt.[21] Daarnaast gaat het om waarborgen waarvoor een wetswijziging nodig is.

Er zij overigens opgemerkt dat profilering en gebiedsgebonden analyses, als vormen van gegevensverwerkingen, aan de voorwaarden uit de AVG en de Richtlijn dienen te voldoen, waaronder het vereiste dat er voor de verwerking een rechtsgrond is.[22] Deze voorwaarden gelden onverkort. Daar ziet deze brief niet op. De in deze brief voorgestelde waarborgen zijn aanvullend op de AVG en Richtlijn.

3.1. Waarborgen met betrekking tot transparantie

Transparantie is een basisprincipe in de AVG (en tot op zekere hoogte ook in de Richtlijn) en is in diverse bepalingen verankerd en nader uitgewerkt. Artikel 5, eerste lid, onder a, bepaalt dat persoonsgegevens verwerkt moeten worden op een wijze die ten aanzien van betrokkenen transparant is. De artikelen 12 tot en met 14 AVG bevatten nadere voorschriften voor de informatievoorziening aan het betrokken individu. Als het gebruik van profilering gepaard gaat met geautomatiseerde besluitvorming, schrijft de AVG voor dat de desbetreffende overheidsdienst de betrokkene informeert dat deze besluitvorming gebaseerd is op profilering en ook nuttige informatie verschaft over de onderliggende logica, het belang en de verwachte gevolgen van die verwerking voor de betrokkene.[23]

Deze informatieverplichting heeft twee beperkingen. Ten eerste is deze verplichting uitsluitend bedoeld om de individuele betrokkenen te informeren, dat wil zeggen de personen van wie persoonsgegevens worden verwerkt.[24] Ten tweede gelden deze bepalingen uitsluitend voor profilering als onderdeel van geautomatiseerde besluitvorming. Dus niet voor profilering als onderdeel van andere vormen van geautomatiseerde gegevensverwerking, vormen die niet in geautomatiseerde besluitvorming uitmonden.

Het kabinet hecht eraan dat geautomatiseerde data-analyses door de overheid zo transparant mogelijk zijn. Transparantie kan immers in belangrijke mate bijdragen aan het vertrouwen dat men in gegevensanalyses door de overheid moet kunnen hebben. Dit geldt temeer nu het

---

[20] Voor zover waarborgen ook gelegen kunnen zijn in de procesrechten van burgers, zullen deze aan bod komen in de kabinetsreactie op het onderzoeksrapport «De modernisering van het Nederlands procesrecht in het licht van Big Data: procedurele waarborgen en toegang tot het recht als randvoorwaarden voor een data-gedreven samenleving», *Tilburg University*. Het kabinet zal voor het eind van het jaar uw Kamer informeren over de conclusies die aan het onderzoeksrapport zullen worden verbonden.

[21] Zo nodig kunnen daarnaast in sectorale wetten aanvullende, voor die sector specifieke waarborgen worden opgenomen. Ook in de EU-Ethics Guidelines for Trustworthy AI wordt voor een dergelijke aanpak gepleit waarbij naast generieke wetgeving, waar nodig, aanvullende sectorale regelgeving wordt vastgesteld.

[22] Dit zijn bijvoorbeeld de noodzakelijkheidseis, het beginsel van doelbinding (art. 5 AVG) en de eisen rond gegevensbeschermingseffectbeoordelingen (art. 35 AVG) en privacy-by-design en privacy-by-default (art. 25 AVG). Zie hierover, overweging 72 AVG en Richtsnoeren, p. 10–22, waarin dit expliciet wordt vermeld en uitgebreid ingegaan wordt op de beginselen en eisen waaraan voldaan moet worden. Het vereiste dat er voor de verwerking een rechtsgrond is, houdt voor overheidsinstanties in de regel in dat het gebruik van profilering noodzakelijk moet zijn ter vervulling van een taak van algemeen belang of om te voldoen aan een wettelijke verplichting.

[23] Artikelen 13, tweede lid, onder f, en 14, tweede lid, onder g, AVG. Hiermee vergelijkbare bepalingen zijn te vinden in de Wjsg (artikel 17a en 17b, derde lid, onder e) en de Wpg (artikel 23 en 24b, tweede lid, onder b).

[24] Een vergelijkbare beperking geldt voor de motiveringsplicht onder de Awb die uitsluitend geldt t.a.v. besluiten in de zin van de Awb en in relatie tot de geadresseerden daarvan.

gebruik van geautomatiseerde data-analyses snel toeneemt en daarmee ook de behoefte om te begrijpen hoe deze processen werken. Transparantie kan ook bijdragen aan controleerbaarheid en daarmee aan de mogelijkheden van burgers om zich te verweren tegen de uitkomst daarvan. Zij is aldus van groot belang voor een effectieve rechtsbescherming van de burger.

i. Informatie aan het publiek

Het kabinet ziet dan ook reden om de bestaande informatieverplichtingen jegens individuele betrokkenen aan te vullen met een bepaling die de informatievoorziening over profilering door de overheid aan het publiek regelt, los van de vraag of men betrokkene is en bovendien geldend voor alle vormen van profilering als bedoeld in de AVG en niet alleen voor profilering als onderdeel van geautomatiseerde besluitvorming. Dezelfde verplichting zou ook moeten gelden voor gebiedsgebonden analyses.

De informatievoorziening zou betrekking moeten hebben op de toepassing en het doel van de verwerking en zou voorts inzicht moeten geven in de verwachte gevolgen van die verwerking voor betrokkenen. Ook zou de informatie duidelijkheid moeten geven over het type gegevens dat wordt gebruikt, en de toepassing van maatregelen ter borging van de kwaliteit van het analyseproces (zie hierna, onder *Kwaliteitswaarborgen*). In het geval dat profilering onderdeel van geautomatiseerde besluitvorming uitmaakt, zou de informatievoorziening bovendien moeten ingaan op de wijze waarop men van het recht op menselijke tussenkomst gebruik kan maken (zie hierna, onder Kwaliteitswaarborgen, sub v). Overheidsorganen zouden deze informatie kunnen opnemen in een privacyverklaring op hun website.

ii. Uitlegbaarheid

Controleerbaarheid impliceert uitlegbaarheid. Daarbij gaat het erom dat de uitkomsten van data-analyses en hoe deze tot stand zijn gekomen, in begrijpelijke taal moeten kunnen worden verklaard aan betrokkenen. Gedacht kan worden aan maatregelen die duidelijkheid geven over het toegepaste model of algoritme, het doel dat daarmee wordt nagestreefd, de procedures die door het algoritme worden gevolgd, de gebruikte datasets inclusief de kwaliteit en herkomst daarvan en de variabelen en/of beoordelingscriteria die doorslaggevend zijn geweest voor de uitkomst. In het verlengde hiervan zou als uitgangspunt moeten gelden dat overheidsorganisaties geen algoritmes mogen hanteren die te complex zijn om redelijkerwijs te kunnen worden uitgelegd.[25]

Anders dan de informatie die aan het publiek wordt verschaft, zal deze informatie in concrete gevallen worden gegeven, bijvoorbeeld op verzoek van betrokkene of van de rechter. De informatievoorziening zal dan ook een verdergaande mate van detaillering moeten behelzen.

---

[25] Een dergelijke voorwaarde is te vinden in de Franse uitvoeringsregeling t.a.v. geautomatiseerde individuele besluitvorming ex artikel 22, tweede lid, onder b, AVG: Pour ces décisions (administratives), le responsable du traitement s'assure de la maitrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer en détail et sous forme intelligible à la personne concernée la manière dont le traitement a été mis en œuvre à son égard. Article 10, 2, Loi nr. 78–17 du 6 janvier 1978, zoals gewijzigd door de Loi nr. 2018–493, du 20 juin 2018. Zie hierover, Malgieri, G., «Right to Explanation and Algorithm Legibility in the EU Member States Legislations – Suitable safeguards for automated decision-making within national implementations of the GDPR », p. 17–18.

iii. Uitzonderingen

Vermeden moet worden dat verschaffing van de hierboven bedoelde informatie (onder sub i. en ii.) kan leiden tot een vorm van *«gaming the system»*. Dit is het verschijnsel dat burgers misbruik maken van de gegeven informatie en calculerend gedrag gaan vertonen, waardoor de effectiviteit van het overheidshandelen nadelig wordt beïnvloed. Daarom zal de informatieverschaffing achterwege moeten blijven, voor zover een algemeen belang als bedoeld in artikel 23, eerste lid, AVG zich daartegen verzet.[26] Het gaat daarbij om belangen als de nationale of openbare veiligheid, economische en financiële belangen met inbegrip van fiscale aangelegenheden, volksgezondheid en sociale zekerheid, de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten en de taken op het gebied van toezicht en inspectie op genoemde terreinen.[27] De overheid moet die uitzonderingen wel neerleggen in wetgeving en daarin die uitzondering goed onderbouwen.

3.2 Kwaliteitswaarborgen

Het kabinet wil, zoals gezegd, ook het risico op fouten en onjuistheden in de gebruikte datasets, algoritmes of methodes, en de mogelijke discriminerende effecten die daaruit kunnen volgen, minimaliseren. Dit kan door kwaliteitswaarborgen te stellen aan het gebruik van met name profilering en gebiedsgebonden analyses.

i. Vooraf/tussentijds te nemen maatregelen

Als uitgangspunt zou moeten gelden dat alleen gebruik wordt gemaakt van algoritmes en analysemethodes die op wetenschappelijk verantwoorde wijze zijn ontwikkeld dan wel wetenschappelijk zijn gevalideerd. Ook dient vooraf de keuze voor een analysemethode gemotiveerd te worden gemaakt in functie van het doel van de analyse.

Daarnaast zouden er technische maatregelen moeten worden ontwikkeld en toegepast die erop gericht zijn onregelmatigheden c.q. discriminerende bias die aanwezig zijn in de datasets of modellen te voorkomen, corrigeren of compenseren.[28] De maatregelen zouden voorts kunnen bestaan uit regelmatige beoordelingen (via testcases) van de datasets of trainingsdata, inclusief de kwaliteit ervan

Bij gebruik van algoritmes van derde partijen wordt verder gedacht aan contractuele maatregelen waarbij geregeld wordt dat het algoritme inzichtelijk wordt gemaakt dan wel ter beschikking wordt gesteld zodat het getest kan worden op nauwkeurigheid en functionele correctheid. Overheidsinstanties blijven immers altijd verantwoordelijk voor de resultaten of beslissingen die door middel van door hen gebruikte algoritmes worden gemaakt.

---

[26] Zie ook artikel 21, tweede lid, Wjsg en 27, eerste lid, Wpg.

[27] Als het gaat om het belang van de nationale veiligheid, laat het Cybersecurity Beeld Nederland 2019 zien dat er een significante dreiging uitgaat van cybercriminelen en statelijke actoren. Zie Cybersecuritybeeld Nederland 2019, Kamerstuk 26 643, nr. 614. Hierom dienen organisaties in te zetten op het versterken van hun digitale weerbaarheid. Door het nemen van gepaste beheersmaatregelen, waar het kabinet op inzet middels de Nederlandse Cybersecurity Agenda, kan dit risico aanzienlijk worden verkleind. Zie hierover de Nederlandse Cybersecurity Agenda (Kamerstuk 26 643, nr. 536), Voortgangsrapportage NCSA (Kamerstuk 26 643, nr. 614). Dit kan uiteraard betekenen dat transparantie achterwege moet blijven.

[28] Dergelijke technische maatregelen zijn volop in ontwikkeling. Zie hierover H. Lammerant, P. Blok & P. de Hert, Big data besluitvormingsprocessen en sluipwegen van discriminatie, NTM/NJCM-bull. 2018/1, p. 1–15. Een voorbeeld betreft het justificeren en falsificeren van tussentijdse resultaten.

ii. Validatie en audits

Andere maatregelen bestaan uit validatie en controle door middel van audits van de resultaten van data-analyses en de daarbij gebruikte algoritmes en modellen.[29] Daarbij gaat het om het controleren of het model of algoritme de beoogde functionaliteit correct uitvoert (validatie), respectievelijk het periodiek toetsen van de nauwkeurigheid van de werking van het model of algoritme (audit).[30] Ook kan het gaan om het controleren welke controlemechanismen de organisatie in het proces heeft ingebouwd. Maatregelen inzake validatie en audits impliceren dat gehanteerde modellen, algoritmes en datasets worden gedocumenteerd, zodat ze achteraf geverifieerd kunnen worden.

iii. Doorlopende toepassing en correctie

De hier bedoelde maatregelen zouden op cyclische basis moeten worden uitgevoerd en zolang de profilering of gebiedsgebonden analyse wordt toegepast. De uitkomst van de testen die in eerdere bedoelde procedures en maatregelen liggen opgesloten, zou moeten worden teruggekoppeld en vervolgens verwerkt in het model of algoritme.[31]

iv. Toetsbaarheid

Waar het bij «uitlegbaarheid» gaat om het in begrijpelijke taal beschrijven van de uitkomsten van de analyse, ziet toetsbaarheid erop dat de uitkomsten daadwerkelijk getoetst kunnen worden. Hiertoe dienen data-analyses als profilering en gebiedsgebonden analyses zo te worden ingericht dat de gehanteerde methode, algoritmes en datasets reproduceerbaar en toetsbaar zijn. Toetsbaarheid richt zich primair op toetsing door de toezichthouder en/of rechter.

v. Menselijke tussenkomst

Profilering kan ook plaatsvinden als onderdeel van geautomatiseerde individuele besluitvorming. In dat geval lijkt het volgens het kabinet aangewezen om betrokkene het recht op menselijke tussenkomst te geven. In de memorie van toelichting bij de UAVG is vermeld dat voor geautomatiseerde individuele besluitvorming anders dan op basis van profilering er geen reden is om menselijke tussenkomst te vergen, omdat dit geen toegevoegde waarde heeft.[32] Ingeval van geautomatiseerde besluitvorming op basis van profilering is die toegevoegde waarde er wel. In dat geval kunnen zich immers de eerdergenoemde risico's voordoen van fouten, onregelmatigheden en vooroordelen waarvan burgers nadeel kunnen ondervinden. Menselijke tussenkomst kan die risico's mitigeren.

---

[29] Afhankelijk van het type algoritme en impact daarvan op individuen kan gekozen worden voor interne dan wel externe audits.

[30] Anders dan bij een gegevensbeschermingseffectbeoordeling (artikel 35 AVG) die een voorafgaande inschatting/beoordeling betreft van de privacy gevolgen van een gegevensverwerking, oftewel een controle *ex ante*, voorziet een audit in een controle *ex post* van de werking van het model of algoritme. Alleen een controle vooraf is onvoldoende om fouten en onjuistheden te minimaliseren.

[31] Richtlijn (EU) 2016/680 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. Deze Richtlijn is geïmplementeerd in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).
Zie hierover ook Richtsnoeren, blz. 33–34.

[32] Kamerstuk 34 851, nr. 3, blz. 120.

Indien de geautomatiseerde besluitvorming noodzakelijk is voor de totstandkoming of uitvoering van een overeenkomst of berust op de uitdrukkelijke toestemming van de betrokkene, geldt op grond van de AVG al dat de verwerkingsverantwoordelijke het recht op menselijke tussenkomst moet waarborgen.[33] Voor het geval dat de geautomatiseerde besluitvorming berust op een specifieke wettelijke grondslag, is niet uitdrukkelijk geregeld dat deze waarborg ook geldt. Wel dat de wetgever in passende maatregelen moet voorzien ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene. Als in dat geval profilering onderdeel van de besluitvorming is, zou het recht op menselijke tussenkomst zo'n maatregel kunnen zijn.[34] Van belang is dat de menselijke tussenkomst betekenisvol dient te zijn. Zo dient deze tussenkomst uitgevoerd te worden door iemand die bevoegd en bekwaam is om het besluit te veranderen en dienen alle beschikbare gegevens daarbij te betrokken worden.[35] Overigens zou voor zo'n geval van besluitvorming een specifieke wettelijke grondslag moeten worden gecreëerd.[36] Vooralsnog bestaat een dergelijke grondslag niet.[37]

Specifiek voor profilering als onderdeel van uitsluitend geautomatiseerde individuele besluitvorming zou voorts als waarborg kunnen gelden dat overheidsorganisaties geen algoritmes mogen hanteren die zichzelf automatisch, dit wil zeggen zonder menselijke controle, aanpassen aan eerder behaalde resultaten.[38]

vi. Verwerking bijzondere persoonsgegevens

Bij profileringstechnieken waarbij gegevens op grote schaal met elkaar worden gecombineerd, kunnen onbedoeld verbanden worden blootgelegd die een aanwijzing geven over iemands gezondheid, geloofsovertuiging, seksuele geaardheid of een ander gevoelig persoonsgegeven.[39] Een voorbeeld hiervan is een studie waarbij Facebook-«likes» gecombi-

---

[33] Zie artikel 22, derde lid, AVG.

[34] Vrijwel alle Europese landen die geautomatiseerde individuele besluitvorming, waaronder profilering, wettelijk hebben geregeld, kozen ervoor om als passende maatregel, het recht op menselijke tussenkomst in te voeren. Dit is het geval in Duitsland, Ierland, Hongarije en België. Het Verenigd Koninkrijk koppelt hieraan het recht om een nieuw besluit te verzoeken dat niet uitsluitend geautomatiseerd wordt genomen. Zie hierover Malgieri, G., «Right to Explanation and Algorithm Legibility in the EU Member States Legislations – Suitable safeguards for automated decision-making within national implementations of the GDPR», p. 9–26.

[35] Vgl. Richtsnoeren, blz. 24–25. Bij de uitwerking van deze maatregel zal moeten worden bezien of – gelet op het bestaan van de bestuurlijke weg (bezwaar en beroep) – het recht op menselijke tussenkomst al dan niet beperkt moet worden tot geautomatiseerde beslissingen die zich niet als «besluit» in de zin van de Awb kwalificeren.

[36] Vgl. artikel 40 Uitvoeringswet AVG en Kamerstuk 34 851, nr. 3, p. 122.

[37] Wel voorziet artikel 7a Wpg, dat in het kader van de implementatie van de Richtlijn is aangenomen, in een wettelijke grondslag voor geautomatiseerde besluitvorming op basis van profilering. Het stelt daarbij als uitdrukkelijke voorwaarde dat er voorzien is in voorafgaande menselijke tussenkomst en in specifieke voorlichting aan de betrokkene.

[38] In een recente uitspraak over de verenigbaarheid van de Franse uitvoeringsregeling t.a.v. geautomatiseerde individuele besluitvorming ex artikel 22, tweede lid, onder b, AVG met de Franse Grondwet heeft de Conseil Constitutionnel geoordeeld dat: «le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en oeuvre à son égard. Il en résulte que ne peuvent être utilisés, comme fondement exclusif d'une décision administrative individuelle, des algorithmes susceptibles de réviser eux-mêmes les règles qu'ils appliquent, sans le contrôle et la validation du responsable du traitement». Conseil Constitutionnel, Décision n° 2018–765 DC du 12 juin 2018, §71. Zie hierover, Malgieri, G., «Right to Explanation and Algorithm Legibility in the EU Member States Legislations – Suitable safeguards for automated decision-making within national implementations of the GDPR », p. 17–18.

[39] M.a.w. gegevens die zelf niet tot bijzondere categorieën gegevens behoren, kunnen hiertoe wel gaan behoren wanneer ze met andere gegevens worden gecombineerd. Zie ook Richtsnoeren, blz. 17–18.

neerd werden met gegevens van een beperkte enquête en vervolgens vastgesteld werd dat onderzoekers in 88% van de gevallen de seksuele geaardheid van mannelijke gebruikers goed hadden ingeschat, in 95% hun etnische afkomst en in 82% of een gebruiker christen of moslim was.[40]

Daarnaast kan het zijn dat profileringsmodellen die uitsluitend gebruik maken van ogenschijnlijk objectieve criteria (variabelen), indirect nadelige effecten hebben voor bepaalde individuen of groepen waarvan het een gegeven is dat die stelselmatig meer of minder dan gemiddeld scoren op een of meer van deze criteria. Dit zou indirect discriminerende gevolgen kunnen hebben voor betrokkenen. Zo blijkt uit een recente studie dat een profileringsmodel dat tot doel heeft om geslachtsneutraal voorspellingen te doen inzake het salaris van professoren, nadelig kan uitpakken voor vrouwen, wanneer het zich uitsluitend baseert op variabelen als functieniveau (i.e. *assistant, associate of full*), opleidingsniveau en anciënniteit. Dit omdat vrouwen in vergelijking met mannen in de regel lager scoren op functieniveau. Met andere woorden, er bestaat een verkapte correlatie tussen het functieniveau en het geslacht. Wanneer hiervoor geen correctie plaatsvindt, kunnen de resultaten van het model indirect in het nadeel van vrouwen uitpakken.[41] Dit voorbeeld heeft weliswaar betrekking op het geslacht, maar is evengoed relevant voor bijzondere persoonsgegevens als bedoeld in de AVG. Een ander voorbeeld betreft de mogelijke correlatie tussen etniciteit en postcodes.[42]

Om deze onbedoelde en ongewenste effecten tegen te gaan kan het juist nodig zijn om bij de ontwikkeling van modellen en methoden relevante bijzondere persoonsgegevens te verwerken.[43] Zo kunnen elementen in het profileringsproces die tot vooroordelen kunnen leiden, worden geëlimineerd en kunnen verkapte tekortkomingen in datasets of modellen worden gecorrigeerd. In een recent experimenteel onderzoek is een model ontwikkeld waarmee aangetoond is dat door gebruik van relevante bijzondere persoonsgegevens als controle-variabele, discriminerende effecten gecorrigeerd kunnen worden.[44] Daarom valt te overwegen om bij de ontwikkeling van modellen en, zo nodig, de uitvoering van maatregelen, zoals onder 3.2, i. en ii. bedoeld, toe te staan dat bijzondere categorieën van persoonsgegevens worden verwerkt, voor zover dat noodzakelijk is om discriminerende effecten tegen te gaan.

---

[40] Kosinski, M., Stilwell, D. en Graepel, T., «Private traits and attributes are predictable from digital records of human behaviour», *Proceedings of the National Academy of Sciences of the United States of America*, http://www.pnas.org/content/110/15/5802.full.pdf, geraadpleegd op 29.3.2017.
Zie voor een vergelijkbaar voorbeeld: H. Lammerant, P. Blok & P. de Hert, Big data besluitvormingsprocessen en sluipwegen van discriminatie, NTM/NJCM-bull. 2018/1, p. 8.

[41] Zie hierover: I. Zliobaite, B. Custers, Using sensitive personal data may be necessary for avoiding discrimination in data-driven decision models, Artif Intell Law (2016) 24: p. 183–201. In deze casus vielen de nadelige effecten voor vrouwen mee omdat het nadeel dat vrouwen ondervonden vanwege het lagere functieniveau deels gecompenseerd werd door een voordeel wat betreft het opleidingsniveau.

[42] Zie hierover: M. van der Sangen, Onderzoek naar eerlijke algoritmes voor beleid, 6-8-2019, https://www.cbs.nl/nl-nl/corporate/2019/32/onderzoek-naar-eerlijke-algoritmen-voor-beleid

[43] Zie in die zin ook: H. Lammerant, P. Blok & P. de Hert, Big data besluitvormingsprocessen en sluipwegen van discriminatie, NTM/NJCM-bull. 2018/1, p. 10–11.

[44] Zie hierover: M. van der Sangen, Onderzoek naar eerlijke algoritmes voor beleid, 6-8-2019, https://www.cbs.nl/nl-nl/corporate/2019/32/onderzoek-naar-eerlijke-algoritmen-voor-beleid.

vii. Kwaliteitseisen aan gebruik van statistiek

In zowel profilering als gebiedsgebonden analyse kunnen behalve het oordeel van experts of uit wet- en regelgeving afgeleide criteria, ook statistische verbanden (correlaties) een grote rol spelen.[45] Standaarden en uitgangspunten die voor statistisch onderzoek zijn ontwikkeld, worden echter niet altijd gehanteerd voor analyses waarmee correlaties worden blootgelegd. Hierdoor kunnen de risico's op fouten, in het bijzonder die van *false positives* en *false negatives* bij profilering en van stigmatisering bij gebiedsgebonden analyses, toenemen.

Om deze risico's te verminderen kunnen bepaalde statistische standaarden en uitgangspunten worden geformuleerd.[46] Daarbij zou aansluiting kunnen worden gezocht bij de standaarden die op Europees en internationaal niveau zijn geformuleerd, zoals de Praktijkcode voor Europese Statistieken.[47] In deze code wordt een aantal principes genoemd die daarin ook verder worden uitgewerkt. De partijen die statistische analyses uitvoeren, moeten:

1. professioneel onafhankelijk en voldoende geëquipeerd zijn,
2. zorgen voor deugdelijke onderzoeksmethoden, beproefde en transparante standaardprocedures en kwaliteitsbeleid,
3. bij hun handelen onpartijdig en objectief te werk gaan,
4. zorgen voor nauwkeurige en betrouwbare onderzoeksresultaten en
5. zorgen voor transparantie en goede controle op hun onderzoek.

4. Toezicht en verantwoording

Mede bepalend voor de effectiviteit van een wettelijke regeling inzake waarborgen voor profilering en gebiedsgebonden analyses met behulp van algoritmes, is dat het toezicht op de naleving daarvan duidelijk geborgd is en effectief is. Daarbij is relevant dat het toezicht op gebruik van algoritmes specifieke kennis en kunde vergt.

Bij profilering en gebiedsgebonden analyses, zoals in deze brief aan de orde en waarbij sprake is van gegevensverwerkingen, hoort het toezicht bij de Autoriteit Persoonsgegevens (AP). Naast de AP kunnen ook andere toezichthouders worden geconfronteerd met het gebruik van algoritmes, voor zover dat gebruik zaken betreft die onder hun toezicht vallen. In dat verband laat het kabinet, naar aanleiding van een recente motie van de leden Verhoeven en Van der Molen, onderzoek doen naar mogelijke tekortkomingen in het huidige toezicht op algoritmes en zal daarbij ook onderzoeken of toezichthouders voldoende zijn toegerust om toezicht op algoritmes te kunnen houden.[48] Ook wil het kabinet de start die al is gemaakt om toezichthouders in een samenwerkingsverband van elkaars expertise op algoritmes en AI te laten leren, verdergaand stimuleren. Deze trajecten zullen ten goede komen aan een effectief toezicht op bestaande en mogelijke nieuwe wettelijke waarborgen inzake profilering en gebiedsgebonden analyses.

---

[45] Veelal zijn de bij profilering en gebiedsgebonden analyses gebruikte variabelen en risico-indicatoren afkomstig uit wettelijke criteria, jurisprudentie alsmede ervaring en praktijk.

[46] Ook in de AVG, bijv. overweging 71, worden statistische procedures genoemd als mogelijke maatregelen die gehanteerd kunnen worden om het risico op fouten te minimaliseren. Zie hierover ook: B.C. van Breda, Profilering in de AVG: nieuwe regels, voldoende bescherming? Computerrecht 2017/154, 223 e.v.

[47] https://ec.europa.eu/eurostat/documents/4031688/9394211/KS-02-18-142-NL-N.pdf/580e523c-85a4-406d-9ad2-9a78f5820fc6.

[48] Kamerstuk 26 643, nr. 610. Dit onderzoek is overigens niet beperkt tot de overheid, maar ziet ook op algoritmegebruik door het bedrijfsleven.

Een ander aspect dat van belang is voor de naleving van wettelijke normen is dat er duidelijkheid is over wie verantwoordelijk is voor het gebruik en de uitkomsten van deze data-analyses. Zoals gezegd, zijn overheidsinstanties altijd verantwoordelijk voor de uitkomsten of beslissingen die door middel van door hen gebruikte algoritmes worden gemaakt en dienen zij hier ook verantwoording over af te leggen. Bij profilering en gebiedsgebonden analyses waarbij sprake is van gegevensverwerkingen, zal deze verantwoordelijkheid toekomen aan de zogenaamde «verwerkingsverantwoordelijke», zoals in de AVG en Richtlijn gedefinieerd en geregeld.

5. Slot

In paragraaf 3 zijn voorstellen voor waarborgen beschreven die volgens het kabinet mogelijk opgenomen kunnen worden in generieke wetgeving. Daarnaast kunnen in sectorale wetten aanvullende, voor die sector specifieke, waarborgen worden opgenomen.[49]

Zoals gezegd heeft het kabinet voor ogen om, in een vervolgtraject, het overleg met relevante overheidsorganisaties voort te zetten om de waarborgen verder uit te werken en te toetsen op hun effectiviteit en uitvoerbaarheid. De uitkomsten daarvan zullen worden betrokken bij een evaluatie van de richtlijnen die kort na de zomer van 2020 zal worden afgerond. Op grond van de resultaten van deze evaluatie zullen de richtlijnen zo nodig worden aangepast of aangescherpt. Met deze resultaten zal ook rekening worden gehouden bij het voorbereiden van eventuele wetgeving met waarborgen die dan voldoende zijn uitgekristalliseerd.

De Minister voor Rechtsbescherming,
S. Dekker

[49] Ook de EU-Ethics Guidelines for Trustworthy AI (zie voetnoot 11) zijn voorstander van een dergelijke aanpak, waarbij naast generieke wetgeving, aanvullende sectorale regelgeving waar nodig wordt vastgesteld.